ABSTRACT

An authentication system that verifies various types of authenticity in regards with a visit by a forwarding agent.

An identity authentication system is composed of an authentication card, a user terminal, and a card reader. Upon insertion of the authentication card into the card reader, the user terminal generates a random number, stores therein the generated random number, and outputs the random number to the authentication card. The authentication card generates encrypted information by encrypting the received random number using an identity certification key having been stored therein, and outputs the generated encrypted information to the user terminal. The user terminal decrypts the received encrypted information using an identity authentication key having been stored therein, and performs an authentication by judging whether or not the decrypting result matches the stored random number.